Association for Information Systems
AIS Electronic Library (AISeL)

2016 Proceedings | SIGED: IAIM Conference

2016

Thinking from Upper-Management Perspective: Using Case Studies in Teaching a Health Information Security Course

Chi Zhang
Kennesaw State University, chizhang@kennesaw.edu

THINKING FROM UPPER-MANAGEMENT PERSPECTIVE: USING CASE STUDIES IN TEACHING A HEALTH INFORMATION SECURITY COURSE

Chi Zhang
College of Computing and Software Engineering
Kennesaw State University
chizhang@kennesaw.edu

Abstract:

Case studies have been found to improve student performance and help students develop problem-solving and decision making skills. The understanding of complexity of information technology, such as information security, relies on a curriculum with hands-on exercises. We used a unique hypothetical case study for a physician's office in a health information security course. By working on the case study in teams, students linked the theoretical topics with practical experience, from strategic policy planning, tactical security planning, operational security planning, to audit standards. Students' feedback shows their positive attitude toward the case study project. Students highly praised the project as exciting and challenging in that they have to act professionally in implementing a security system with a low failure rate. This paper reports our experience of using the case study exercises and discusses the potential improvement when using them again in the future.

Keywords: Case study, Health information security and privacy, HIPAA, Course design

I. INTRODUCTION

Numerous studies have shown that using case studies improves student performance and help students develop problem-solving and decision making skills. Prior studies have found that using case studies help students to enjoy the experience, have better attitudes toward the subject and develop better communication and social skills through the cooperative teamwork [Davis and Wilcock, 2003; Ganiron Jr, 2014; Johnson and Johnson, 1989, 1993; Stahli, 2006].

Case studies refer to student-centered activities based on topics that demonstrate theoretical concepts in an applied setting [Davis and Wilcock, 2003]. Real-world cases have been used for many years in the curricula [Boston University, 2015; Stahli, 2006; Standford Graudate School of Business, 2015; University of Virginia School of Medicine, 2015]. In order to work through a case study, students take the hypothetical roles, evaluate the information provided in the case and plan the solution with justification. Instructors have been finding that a case study can help them assess students' ability to synthesize, evaluate, and apply information and concepts learned in lectures [Boston University, 2015].

The understanding of complexity of information technology, such as information security, relies on a curriculum with true hands-on [Mallard, 2010]. With case-based teaching, students develop skills in analytical thinking and reflective judgment by reading and discussing complex, real-life scenarios. Case study problems and real-world scenarios have been used in information security texts [Dhillon, 2007; Katerinsky et al., 2011; Schembari ,2011].

A health information security & privacy course taught at a regional southeastern university in the US introduces the theoretical topics on information security management and how they are applied in healthcare facilities. To help students link the theoretical topics with practical experience, we researched and found a NSF-funded project [Lincke, 2012] that provides a hypothetical case study for a physician's office. It covers strategic policy planning, tactical security planning, operational security planning, and audit standards.

The Students in the health information security & privacy course worked on a set of selected case study exercises in teams in both the summer term of 2015 and 2016. Students' feedback on the

case studies was collected and analyzed. The paper is organized as follows: the information security case study in the context of healthcare is introduced in section two. The practitioners' views on the course, the process of the case study exercises are discussed in section three and four. Students' feedback is reported in section five, followed by the discussion and appendix.

II. PRACTIONERS VIEWS ON A HEALTH INFORMATION SECURITY COURSE

To prepare for the Health Information Security & Privacy course, the instructor consulted the Industrial Advisory Board (IAB) of the Department of Information Technology. As the experienced IT professionals and mangers, the IAB members help assess the IT courses and offer insights into the current and emerging IT trends. They also inform the faculty the technical skills that IT graduates should have. Bringing their experiences working in the industry into the instructor's research and preparation work, here is what was planned for a HIT Security course:

1. NIST Cybersecurity Framework: What is NIST; what is the cyber security framework; and How do you use the Framework
2. What is a risk: How do you write a risk: why do organizations care about risks (why are risks important – i.e. as a tool to manage uncertainty)
3. Risk assessment: What is a risk assessment; how do you perform a risk assessment; and how do you use a risk assessment
4. Risk management plan: What is a risk management plan; how do you make a risk management plan; and how do you use a risk management plan
5. HIPAA Security Rule: What is it; how does it apply to Providers; and how does it relate to Meaningful Use
6. Risk Assessment tools: ONC Risk Assessment Tool and NIST HIPAA Security Toolkit
7. Risk certifications: What are the different risk certifications that are available and what are the requirements for each one

The IAB members also pointed out that in addition to the topics above, the course should have a project that provides a vehicle for the students to put the learning to practice. One possible project would be to apply the topics to a real-world case. In other words, the purpose of the project would be to run a risk assessment on a real-world physician's office and come up with a risk management plan – the same way a doctor's office would. The project would involve such things as

- Creating an inventory of all devices
- Identifying where their data is
- Identifying the different users
- Identifying potential risks
- Identifying mitigations

When the project was completed, students should be able to explain all the steps and deliverables that a Healthcare org would do – and provide concrete examples based on the student's own home. The project and its deliverables would provide the students a means to show their knowledge of the topics in job interviews. The project and deliverables would also serve as a handy vehicle for a student to go back and brush up on the key topics at a later date.

III. OVERVIEW OF THE HEALTH INFORATION SECURITY CASE STUDIES

Lincke [2015] developed a series of case study exercises for undergraduate Computer Science, Information Systems, and Information Technology students to plan security for a doctor's office. In the US, many doctor's offices or clinics are considered small businesses, as the Health First clinic

introduced in the case study. These clinics must also adhere to federal laws governing privacy and security of patient information including the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its related security and privacy rules.

To help the students work through the case studies, a Security Workbook has been developed by [Linkre, 2015] that guides small businesses through the process of organizing a security program. The Security Workbook provides a procedure for building security plans for a generic small business. In combination, the Health First Case Study and Security Workbook introduce a realistic organizational setting.

The Health First project helped students develop security in a real world environment by working through the case study security workbook. After studying the package of the case study, we found out that the exercises would be a great addition to the course of Health Information Security & Privacy because it provides the unique cases in the context of healthcare.

The topics covered in the case study exercises include:

1. Strategic Policy Planning (risk analysis, business impact analysis & business continuity, legal compliance, policy manual)
2. Tactical Security Planning (network security plan, physical security plan, incident response, personnel security plan, metrics)
3. Operational Security Planning (computer & server security, network security, physical security, business continuity, personnel security)
4. Audit Standards (audit planning, audit plan standard, audit report standard, equipment baseline audit)

The case study not only provides the scenarios and problems but also the knowledge base for solving the problems. The case study project is based on ISACA's COBIT, NISTIR 7621 and other professional security guides (CISA, CISM) [Linkre, 2015]. The case study exercises are closely related to the theoretical topics introduced in the course including security management, risk analysis, and HIPAA.

IV. SELECTED CASE STUDY EXERCISES FOR THE HEALTH INFORMATION SECURITY COURSE

Due to the time constraint in the summer term, the following exercises addressing the two areas were selected as a team project for the course:

1. Management areas require decisions to be made at the top management level, which provide direction based on business needs:
    1) Risk Analysis: What risks could cause substantial damage to the organization? This section evaluates, documents, and addresses such risk.
    2) Business Impact Analysis: If a computer server or network goes out-of-service, how would the organization cope? Which business functions cannot be manually done in an emergency? Data would be lost if a disk failure occurred: for how long (or for what duration) can the organization afford to lose data?
    3) HIPAA Adherence: HIPAA compliance is a necessary aspect of being in the medical profession. What are the standards for privacy rule implementation, patient's rights, and PHI disclosure?
2. Tactical areas:
    1) Information Security: Which data is of strategic or critical importance? Which data must remain confidential for legal, liability, business competition, trade secret, goodwill or reputational reasons? Data must be categorized and procedures must be defined for how each category of data is to be handled.

Secondly, who should have access to confidential or critical data? How is authorization to be handled to ensure access is limited?

2) Incident Response: If an attacker does enter the organization's computer network, how should IT respond: close down the system immediately or continue operation? Should law enforcement be called in? When should management be notified? A list of actions to be taken in such an event is defined.

3) Metrics: Metrics ensure that compliance to policies and security control is effective. This is a scorecard of the security program

Each of the above topics are introduced to the students before they started to work on the project. For example, the sub-topics: risk management, risk assessment, risk analysis, risk treatment, accept residual risk for the topic of risk management process; risk acceptance/risk retention, risk avoidance, risk mitigation/risk reduction, risk transference for the treat risk terms; natural, unintentional, intentional, non-physical intentional for the threat types; hacker/crackers, criminals, terrorists, industry spies, insiders for the threat agent types; and the definitions of vulnerability, single loss expectancy, annualized rate of occurrence, annual loss expectancy, due diligence, and due dare. The project details on analyzing risk can be found in Appendix A for illustration.

Students were guided to study the lectures on the topics in each of the two areas including HIPAA, risk analysis, business continuity, and security management before reading through the case study and starting the work on solving the problems. They are required to submit a project experience reflection in addition to completing the project. The open-ended questions for the project experience reflection are:

1) Please describe your experience with the team project.
2) What have you learned from working on the project?
3) Did you have any difficulties when working on the project?
4) How well did your team work on the project? Who worked on which part of the project?
5) Do you have any suggestions and comments for the future run of this project?

V. STUDENT FEEDBACK

Fifteen students in summer 2015 and twenty-three students in summer 2016 who had participated in the case study exercises submitted their personal reflection on their experience of the project. They found the project "exciting, challenging, and interesting". They appreciated the exciting opportunity for them to act as real world security officer implementing guidance for a well-structured organization where the implemented procedures will enhance the organization core measures. Students also praised the project as challenging in that they have to act professionally in implementing a security system with a low failure rate (because it is a healthcare facility). Lastly the project was interesting in that it helped students to foster their ability to interact with people. A selectin of students' quotes on their overall experience, what they had learned from the project, the difficulties they had encountered is as follows:

Overall Experience

The students reported their satisfaction of the real-life case interesting and helpful for their future careers in IT or any management role in the future because the project forces them to think outside the box.

- Health First case studies required me to think about each of the three components of (health) information security, and actually apply them to a real-life situation, which I always enjoy, as somebody already in the workforce. I had to think what were the most important parts of my business to continually operate, and the cost of not having those consequential parts, and the possible mechanisms to work around that.

- I found the project pretty interesting, as it was a new experience for me to attempt to determine the types of assets a hospital would have, the value of those assets, and different risks that a clinic may face from everything to the elements to network problems.
- I feel that this Case study will help me in future to solve issues in real world. Completing this project has been a nice experience in this semester.
- The project itself was very interesting. The high point of the project was its real world value. It allowed evoking our imagination to real world situations. That is a great learning curve as it makes the students ready for the stepping in the work zone.
- It was very in-depth and way more than I have ever been asked to do in my IT career concerning security.
- The case study was a good reflection of a real life situation especially dealing with security for a real world environment. By applying those areas learnt in class to the project, it makes it more clear and memorable.
- Overall the experience was outstanding, by learning a lot of terms and by improving the knowledge with additional info from Heath IT. I did found out how important are the data in any division and organization, ho the Business Process are working differently and witch one is priority.
- I think this project is really helpful for somebody pursuing any sort of IT role, or even any Management role in the future, because it forces you to think outside the box, and consider many situations, regardless of how likely or unlikely they are.

How the project helped student learning?

The project helped students better understand the concepts of risk assessment, the process of risk planning, the development and implantation of the procedures in compliance of HIPAA, and the responsibilities of the information security officer.

- I have a better understanding of how to properly assess risks in a business scenario. This project taught me how to better analyze possible risk to a business, and how to figure out proper ways to mitigate those risk.
- The project walked me through the whole process of brainstorming, planning (practically, financially, and legally), and creating backup plans for a proposed plan.
- I learned a lot on how the security officer responsibilities are impacting the organization, the steps need to follow and the values.
- I learned a lot on how the security officer responsibilities are impacting the organization, the steps need to follow and the values. By doing the project and learning the case study I was able to see a lot of opportunity in this field for the security officer
- Now, I am confident on developing and implementing procedures that tie with HIPAA policies and procedures. The project helped me to have a better understanding of the material covered in the slides.

Difficulties reported

The students did report difficulties that they had encountered with a couple of steps of the projects that are new to them, and with their teammates as in any other team projects.

- Communication difficulties with team members.

- I had some difficulty assigning the correct value to assets, as well as the correct value when risks such as fire were involved.
- The project took a lot of time to read and understand. I was confused on many occasions as to whether I needed to come up with new business processes and threats.

The students' overall experiences with the case studies are positive and encouraging.

VI. DISCUSSION

It has been found that the Health First case study exercises enable to students understand better the topics covered in the course of Health Information Security & Privacy. As a student, finding and working with a physician's office is a challenge. The case study approach helps enhance students learning. The team project, on the other hand, let students collaborate with peers to work on a relatively large-scale project.

Potential improvement could be made when using the case study next time in the course, such as adding smaller exercises throughout the semester; reminding student teams to have clear communication among team members and ability to work independently, delineating specific responsibilities and setting up specific internal deadlines.

The case study method in teaching provides a practical learning process with the cases reflecting real-world situations. The Health First project helped students to develop security in a real world environment by working through the case study security workbook. The success of the project shows that students are able to appreciate the teamwork, the real-world problems, and the opportunity to understand deeply the theoretical concepts, different perspectives of team members, and think outside the box – to think from an upper-management perspective – a Director or executives, but also from a working-level Security Analyst as well. The success of the case study project also demonstrates that the importance of the practitioners views on the course design and development. We found that the twice-a-year IAB meetings are beneficial for our IT programs.

VII. ACKNOWLEGEMENT

This research was supported by the Center for Excellence of Teaching and Learning at Kennesaw State University, the Incentive Funds for Research and Creative Activity. I thank Dr. Susan Lincke at the University of Wisconsin Parkside for her generous help and innovative work on the Health First Clinic case study. I would also like to thank the IAB member Mr. Mike Boucher, the program manager at NextGen, who provided insights and expertise that greatly assisted the development of our Health IT courses.

VIII. REFERENCES

Boston University. (2015) Using Case Studies to Teach » Center for Excellence & Innovation in Teaching | Boston University. Retrieved February 25, 2015, from http://www.bu.edu/ceit/teaching-resources/using-case-studies-to-teach/.

Davis, C., & Wilcock, E. (2003) Teaching Materials Using Case Studies. Retrieved from http://www.materials.ac.uk/guides/1-casestudies.pdf.

Dhillon, G. (2007) Principles of Information Systems Security: Texts and Cases. Wiley.

Ganiron Jr, T. U. (2014) The Impact of Higher Level Thinking on Students' Achievement toward Project Management Course. International Journal of U - and E - Service, Science and Technology, 7(3), 217–226.

Johnson, D. W., & Johnson, R. T. (1989) Cooperation and competition: theory and research. Interaction Book Co.

Johnson, D. W., & Johnson, R. T. (1993) Cooperative learning: Where we have been, where we are going. Cooperative Learning and Teaching Newsletter, 3(2), 6–9.

Katerinsky, A., Rao, H. R., & Upadhyaya, S. (2011) Harsh Realities 101 - Augmenting Information Assurance with Legal Curricula. In Proceedings of 14th Colloquium for Information Systems Security Education (CISSE).

Lincke, S. J. (2012) The Health First Case Study: Teaching HIPAA Regulation with Security Planning. In Proceedings of the 16th Colloquium for Information Systems Security Education. Lake Buena Vista, FL.

Lincke, S. J. (2015) *Security Planning: An Applied Approach*, *2015 edition*, New York: Springer Publishing Company.

Schembari, N. P. (2011) An Active Learning Approach for Coursework in Information Assurance Ethics and Law. In Proceedings of 14th Colloquium for Information Systems Security Education (CISSE).

Stahli, A. (2006) From the Harvard Case Study Method to the Genetically Growing Case Study. In Management Andragogics 2 (pp. 3–11). Springer Berlin Heidelberg. Retrieved from http://link.springer.com/chapter/10.1007/3-540-28975-5_1.

Standford Graudate School of Business (2015) Case Studies. Retrieved February 25, 2015, from http://www.gsb.stanford.edu/faculty-research/case-studies.

University of Virginia School of Medicine (2015) Case Studies — School of Medicine at the University of Virginia [Folder]. Retrieved February 25, 2015, from http://www.medicine.virginia.edu/clinical/departments/pathology/Case%20Studies.

APPENDIX A

Workbook for Analyzing Risk

Vocabulary:

The three major components of security to consider when working with risk include:

Confidentiality: Data or resources are available only to authorized parties.

Integrity: Data or resources are complete, accurate, and functional.

Availability: Data or resources are available to be used when needed.

Security and privacy regulation demands:

Due Diligence: Perform a thorough and objective analysis of risk in a careful and responsible manner.

Due Care: Implement recommended and sufficient controls, as would be addressed by a reasonable person of similar competency under similar conditions.

The ultimate decision(s) of how risk should be managed is the prerogative of executive management. The steps of risk analysis include:

Step 1: Determine Value of Assets (Crown Jewels):

The first step in risk analysis is to evaluate the value of the organization's assets. Assets should be **prioritized,** with most important assets considered. Assets include:

IT-Related: Information/data, hardware, software, services, documents, personnel

Other: Buildings, inventory, cash, reputation, sales opportunities

Direct Loss considers replacement costs:

How much would it cost to replace this asset? (Consider purchase, installation, recovery)

Consequential Financial Loss considers:

How much of our income can we attribute to this asset?

How much liability would we be subject to if the asset was compromised?

What intangibles would we risk? Goodwill, reputation, future business?

Does this asset have other value to the company?

SLE = Single Loss Expectancy = The cost to the organization if one threat occurs once

= Replacement Cost + Consequential Cost

Consequential Cost = liability/defense/goodwill + loss of business

Below are some sample starter values you can modify, add to, or delete.

Table 3.3.1: Asset Value Table

Asset Name	$ Value Direct Loss: Replacement	$ Value Consequential Financial Loss	Confidentiality, Integrity, and Availability Notes
Building		1D	Availability
Database		NL	Integrity, Availability

You may include notes about the Consequential Financial Loss below:

Table 3.3.2: Consequential Financial Loss Calculations

Consequential Financial Loss	Total Loss	Calculations or Notes
Lost business for one day (1D)		Insert '1D x Duration' in Consequential Financial Loss above
Privacy breach notification liability (NL)		
Lawsuit (L)		

Step 2: Estimate Potential Loss for Threats:

The second step is to determine the threats that could affect these assets. Threats that should be considered are listed below. **Circle the threats that are most important to your organization. Add threats specific to your industry as appropriate.**

Normal threats: Threats common to all organizations

Inherent threats: Threats particular to your specific industry

Known vulnerabilities: Previous audit reports indicate deficiencies.

Here are some categories and specific threats to consider:

Physical Threats

- Natural: Flood, fire, cyclones, hail/snow, plagues and earthquakes

- Unintentional: Fire, water, building damage/collapse, loss of utility services and equipment failure
- Intentional: Fire, water, theft and vandalism

Non-Physical Threats

- Ethical/Criminal: Fraud, espionage, hacking, identity theft, malicious code, social engineering, vandalism, phishing and denial of service
- External Environmental: industry competition, contract failure, or changes in market, political, regulatory or technology environment
- Internal: management error, IT complexity, poor risk evaluation, organization immaturity, accidental data loss, mistakes, software defects and personnel incompetence.

Possible threat agents include people who perform intentional threats, such as: crackers, criminals, industry spies, insiders (e.g., fraudsters), and terrorists/hacktivists

Vulnerabilities are the 'open doors' that enable threats to occur. Categories of vulnerabilities include*:*

- Behavioral: Disgruntled employee, poor security design, improperly configured equipment;
- Misinterpretation: Employee error or incompetence, poor procedural documentation, poor compliance adherence, insufficient staff;
- Poor coding: Incomplete requirements, software defects, inadequate security design;
- Physical vulnerabilities: theft, negligence, extreme weather, no redundancy, violent attack.

Document your normal and inherent threats and known vulnerabilities in Figure 3.2.1 and Table 3.3.3.

Step 3: Estimate Likelihood of Exploitation

Once we have listed the threats, we must determine the probability that they will occur. This is best evaluated using historical data, published figures, or if no figures are available, best guesses.

> Is this likely to occur monthly, 1 year, 10 years, 20 years, 50 years?
>
> Calculate **Annual Rate of Occurrence (ARO)** = How many times this is likely to occur in one year

The likelihood of each threat is documented in Figure 3.3.1 and Table 3.3.2. In Figure 3.3.1, be sure to include all threats, with estimated potential likelihood. It is possible to move the threats around that exist in the current diagram. It is also possible to expand the size of the diagram to consider all threats.

This table shows example values for some threats. The table can be expanded and modified as needed. Observe the time frame on the left side, and the impact levels on the top.

Step 4: Compute Expected Loss

The next step is to prioritize the risks, according to their severity of impact. To accomplish this, it is best to calculate an annualized loss expectancy, using the Quantitative method in Table 3.3.3. If this is not possible, expected loss can be prioritized by using Figure 3.2.1 Qualitative Analysis of Risk. Relevant Quantitative equations include:

> **Single Loss Expectancy (SLE)** = The cost of a single problematic event = Downtime + Recovery + Liability + Replacement

Annual Rate of Occurrence (ARO) = the probability or likelihood that that a SLE might occur during one year

Risk Exposure or **Annual Loss Expectancy (ALE)** = expected loss per year due to the threat = $_Loss * Probability(Vulnerability) = SLE x ARO

For example:

SLE (PC failure) = $1000 replacement + $1000 lost salary = $2000

Probability (PC failure) = once in 8 years = 1/8 or 12.5%

ALE (PC failure) = 0.125 x $2000 = $250 per year.

Table 3.3.3: Quantitative Risk Loss Table

Asset	Threat	Single Loss Expectancy (SLE)	Annualized Rate of Occurrence (ARO)	Annual Loss Expectancy (ALE)

Step 5: Treat Risk

Once the risks are prioritized, we can treat the high priority risks, and accept the low priority risks. The steps include:

Survey & Select New Controls: Technical, managerial, or operational controls

Reduce, Transfer, Avoid or Accept Risk

Risk Acceptance: Handle attack when necessary

E.g., a comet hits

Ignore risk if risk exposure is negligible

Risk Avoidance: Stop doing risky behavior

E.g., do not use Social Security Numbers

Risk Mitigation: Implement control to minimize vulnerability

E.g., purchase & configure a firewall

Risk Transference: Pay someone to assume risk for you

E.g., buy malpractice insurance (doctor)

While financial impact can be transferred, legal responsibility cannot

Risk Planning: Implement a set of controls

Risk Leverage = (Risk exposure before reduction) – (risk exposure after reduction) / (cost of risk reduction)

The decision of how much risk to mitigate or accept is an executive management decision. Risk and controls should be addressed in Table 3.2.4: Analysis of Risk versus Controls.

Question: What approach to security controls is planned, and why?

Table 3.3.4: Analysis of Risk versus Controls

Risk	ALE Score	Control	Cost of Control